Deutscher Bundestag
13. Wahlperiode

Drucksache 13/4391

17. 04. 96

Kleine Anfrage

des Abgeordneten Dr. Manuel Kiper und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Kontrolle und Selektion von Telekommunikationsvorgängen

Das Internet ist ein vielfältiges neues elektronisches Medium des Datenaustauschs. Es bietet Weltfirmen wie Privatpersonen in annähernd gleicher Weise die Möglichkeit, ihre Ansichten zu verbreiten, Informationen zur Verfügung zu stellen und damit zu weltweiten Informationsanbietern zu werden.

Dies machen sich auch Anbieter zunutze, die sich nicht an die in der Bundesrepublik Deutschland herrschenden Gesetze halten. Rechtsradikale bieten ihre gesetzwidrige Hetzpropaganda auf Computern in solchen Staaten an, in denen deren Verbreitung straffrei ist. Selbst Daten mit kinderpornographischen Inhalten werden auf dem Internet beworben und angeboten, obwohl dies in den meisten Staaten verboten ist. Mit dem Abruf derartigen Materials aus Mailboxen werden Geschäfte gemacht.

Die Verfolgung von Straftaten, die mit Hilfe elektronischer Netze wie dem Internet verübt werden, ist legitime Aufgabe der Strafverfolgungsbehörden. Ihre Arbeit wird jedoch durch den weltweiten Charakter des Internets erschwert. Die Ermittlung von Tätern ist nicht an Orts- oder Landesgrenzen gebunden. In der Politik wurden bisher vor allem wirtschaftliche Aspekte behandelt, kaum dagegen die Probleme, die aus dem Vernetzen der Rechtskulturen der ans Internet angeschlossenen Staaten und damit dem elektronischen Kurzschluß der zahlreichen verschiedenen Rechtssysteme erwachsen.

Einigkeit wird sich bei der Verfolgung schwerwiegender Straftaten erzielen lassen, die mit Hilfe elektronischer Kommunikationsnetze verübt wurden. Bei Kommunikationsnetzwerken beschränkt sich jedoch die Mehrzahl der Delikte auf Meinungsäußerungstatbestände, deren Zulässigkeit nicht einmal in klassischen westlichen Demokratien einheitlich gehandhabt wird.

Die Konferenz der G7-Staaten 1995 zur Weiterentwicklung einer globalen Informations-Infrastruktur hat sich nicht darauf geeinigt, rechtsstaatliche und demokratische Prinzipien auf dem Internet umzusetzen. Die Frage der Meinungsfreiheit wurde damit nicht einmal als Absichtserklärung umrissen. Rechtliche Konflikte entstehen auf der bestehenden Informations-Infrastruktur so durch

die elektronische Verbreitung strafbarer Daten, deren Strafbarkeit unterschiedlich bewertet wird, und von Meinungsäußerungen, die in einigen Staaten straffrei, in anderen strafbewehrt sind.

Selbst in der Bundesrepublik Deutschland gibt es keine einheitliche Rechtsauffassung zu den mittlerweile typischen Internet-Diensten. Die Bundesregierung vertrat die durchaus plausible Auffassung, der Schutz der Jugend vor Gewalt und Pornographie sei durch die bestehenden Gesetze gewährleistet, ihr seien die Kommunikationsinhalte auf Datennetzen jedoch nicht bekannt, da es sich dabei um eine durch das Fernmeldegeheimnis geschützte Individualkommunikation handele (Drucksache 13/2205, Frage 13). Staatsanwaltschaften haben dagegen Anbietern von Internet-Zugängen – Internet-Providern – die Verantwortung für die Inhalte ihrer Angebote zugeordnet. Diese Auffassung hat die Bundesregierung selbst in der Folge vertreten (Drucksache 13/4036, Frage 42).

Daraus folgt der Widerspruch, daß Internet-Provider entweder für die Inhalte der von ihnen verteilten Daten verantwortlich sind und deshalb die Kommunikation ihrer Kundinnen und Kunden auf möglicherweise Strafbares kontrollieren müssen oder das Fernmeldegeheimnis achten, daher die Kommunikationsinhalte ihrer Kundinnen und Kunden nicht zur Kenntnis nehmen, dafür aber zur Verantwortung gezogen werden.

Eine Differenzierung zwischen Individual- und Massenkommunikation, die Entscheidungshilfe in diesem Dilemma bieten würde, hat die Bundesregierung mit ihrem Multimediagesetz angekündigt, doch ist auch dadurch nicht zu erwarten, daß dies angesichts der Vielfalt der Angebotsformen elektronischer Kommunikation abschließende Rechtssicherheit gibt. Die Bundesregierung hätte jedoch nicht nur nationale Gesetze zu modifizieren, sondern auch darauf zu achten, die von ihr unterzeichneten internationalen Abkommen und Verträge über den freien Zugang zu Informationen zu erfüllen.

Die Initiative bei der Setzung von Recht ging jedoch in den letzten Monaten von den Strafverfolgungsbehörden aus. Als lokales Mittel gegen den weltweit und verteilt ablaufenden elektronischen Datenaustausch haben Strafverfolgungsbehörden in der Bundesrepublik Deutschland zunächst die Firma CompuServe als Internet-Provider bewogen, den Zugang zu einigen sogenannten Internet-Newsgruppen zu sperren, bei denen die Staatsanwaltschaft München die Verbreitung von strafbarer Pornographie vermutete. In Newsgruppen werden im allgemeinen Beiträge beliebiger Abonnentinnen und Abonnenten der jeweiligen Gruppe ohne zentrale Steuerung und ohne inhaltliche Selektion über das gesamte weltweite Netz verteilt. Die Sperrung des Gruppenzugangs ist jedoch nur Mittel für Provider, die wie CompuServe den Internet-Zugang zentral organisieren. Die Urheber der inkriminierten Daten und damit die eigentlichen Straftäter werden dadurch nicht getroffen, sondern die Übermittler der Daten. Sie können jedoch eine inhaltliche Rechtskonformitäts-Kontrolle der Daten bei den erreichten Übertragungsmengen – abgesehen von

den juristischen Problemen – weder technisch noch organisatorisch leisten. Das Unterdrücken von Newsgruppen ist jedoch einem Verbot gleichzusetzen, dessen rechtliche Zulässigkeit ohne einen Beschluß der Bundesprüfstelle für jugendgefährdende Schriften oder eines Gerichts fraglich ist.

Ein anderes lokales Mittel gegen eine andere Klasse von Internet-Diensten war das Sperren des Zugangs von bestimmten Angeboten im World Wide Web, bei denen rechtsextremistische Propaganda angeboten wird. Dies wurde aufgrund staatsanwaltschaftlicher Ermittlungen von einigen Providern durchgeführt. Dies führt zu einem weiteren Rechtsproblem. Das World Wide Web (WWW) ist ein hypermedialer Datenabruf-Dienst, bei dem die logische Internet-Adresse des jeweiligen Computers anzuwählen ist, um die gewünschten Daten zu beziehen. Die Adressierung basiert darauf, daß einem Computer im Internet ähnlich einem Telefonanschluß ebenfalls eine Nummer zugeordnet ist, über die dieser angesprochen werden kann. Mit der Nutzung digitaler Telekommunikationstechnologie, die zur virtuellen Zuordnung von Telefonnummern bei Anrufweiterschaltung und anderen Diensten geführt hat, ist eine solche Adresse insoweit mit Telefonnummern technisch gleichzusetzen, als in beiden Fällen eine elektronisch vermittelte Verbindung zwischen zwei Kommunikationspartnern aufgebaut wird. Dabei ist unerheblich, auf welchem Weg dies physikalisch realisiert wird.

Die elektronische Adressierung von Computern auf Umwegen und die direkte Anwahl von Computern per Telefon sind einfache Methoden, um eine Sperrung einzelner Internet-Angebote zu umgehen. Sie führen in logischer Konsequenz jedoch zu der Forderung, auch andere Zugangswege zu inkriminierten Daten zu verbauen. Die Sperrung von Angeboten im World Wide Web wird somit zum Präzedenzfall für die technisch wie rechtlich kaum zu differenzierende Möglichkeit einer Sperrung von Telekommunikationsdienstleistungen allgemein. Mit den durch digitale Vermittlungsstellen anfallenden Verbindungsdaten liegen Informationen vor, die nutzbar sind, um das Zustandekommen einer Verbindung etwa zu den typischerweise mit Anrufbeantwortern arbeitenden rechtsextremistischen Informationsdiensten zu unterbinden. Seitdem die Post AG in ihren Briefzentren durch Anschriften lesende Computer die Möglichkeit hat, Sendungen maschinell auszusortieren und von einer Zustellung auszunehmen, ließe sich ein solches automatisches Selektieren sogar auf die auf dem Postweg beförderten Sendungen ausweiten.

Eine Selektion von Telefonnummern fand in der Bundesrepublik Deutschland bislang allenfalls insofern statt, als die Telekom AG die Anwahl von solchen Ansagediensten auf Handvermittlung umgestellt hat, bei denen sie einen Gebührenbetrug zu ihren Lasten vermutete. Eine effektive Sperrung ist dies jedoch nicht. Die vollständige Digitalisierung des Telekom-Netzes könnte dies aber ab 1998 automatisiert und flächendeckend ermöglichen. In den USA wird die fallweise Unterdrückung von Nummern verschiedentlich als Serviceübereinkunft zwischen Telefonunternehmen und Kunde angeboten.

Die Sperrung von Kommunikationsmitteln entspräche auch der Forderung nach einer Zugangskontrolle für technische Mittel wie Mailboxen, Anrufbeantworter und Mobiltelefone für politische Extremisten, die im Herbst 1993 von den Präsidenten des Bundeskriminalamtes und des Bundesamtes für Verfassungsschutz sowie vom damaligen Staatssekretär des Bundesministeriums des Innern erhoben wurde. Unerwähnt blieben damit als Informationsform lediglich Faxabrufdienste, die sich funktional jedoch kaum von Mailboxen oder Anrufbeantwortern differenzieren lassen. Die in der Politik erhobene Forderung nach Zugangskontrolle, ihre technische Realisierbarkeit und die erfolgte Anwendung beim WWW-Dienst widersprechen nicht nur dem Schutz des Post- und Fernmeldegeheimnisses, sondern heben auch die Freiheit des Individuums, sich eine eigene Meinung zu bilden und per Post oder auf telekommunikativem Wege mit Personen seiner Wahl zu kommunizieren, auf.

Wir fragen die Bundesregierung:

1. Wie hoch ist nach Ansicht der Bundesregierung die pro Tag anfallende Menge von Daten bei den auf dem Internet verfügbaren Diensten sowohl bei großen Internet-Knotenrechnern als auch bei Internet-Providern, die in der Bundesrepublik Deutschland ihre Dienste anbieten?

2. Welche Form von elektronischer Kommunikation – E-Mail, Internet-News und Mailbox-Bretter, Dateien-Transfer in verschiedenen Formen sowohl im Internet als auch bei Mailboxen sowie World Wide Web-Nutzung – ist nach Auffassung der Bundesregierung Individualkommunikation, welche nicht, und bei welcher handelt es sich um Massenkommunikation?

3. In welcher Weise sollen Internet-Provider die Inhalte von Individualkommunikation kontrollieren, und wie kann dies nach Ansicht der Bundesregierung ohne Verstoß gegen das Fernmeldegeheimnis geschehen?

4. In welcher Weise sollen nach Ansicht der Bundesregierung Internet-Provider die Inhalte der von ihr als Massenkommunikation klassifizierten Internet-Angebote kontrollieren?

5. Auf welche Rechtsgrundlage bezieht sich diese Ansicht?

6. Sieht die Bundesregierung bei den vorhandenen Formen elektronischer Kommunikation solche, die weder unter den Begriff der Individual- noch unter den der Massenkommunikation zu fassen sind, und welche Regelungen hält sie bei diesen für notwendig?

7. Inwieweit muß nach Ansicht der Bundesregierung bei der Regelung von elektronischer Kommunikation in die Medienhoheit der Bundesländer eingegriffen werden?

8. Gilt die Auffassung der Bundesregierung zur Kontrolle von Inhalten elektronischer Kommunikation nur für das Verfügbarmachen von Daten für Kundinnen und Kunden der Provider oder auch für das Durchleiten von Daten?

9. Hat sich die in der Antwort auf eine schriftliche Frage zur Internet-Kommunikation gegebene Ansicht der Bundesregierung (Drucksache 13/2205, Frage 13) zur Reglementierung von Telekommunikationsinhalten geändert?

   Wenn ja, in welchem Umfang, in welcher Hinsicht und wie begründet die Bundesregierung dies gegebenenfalls?

10. Wie hoch schätzt die Bundesregierung die Zahl von Internet-Newsgruppen und World Wide Web-Angeboten, und wie hoch ist davon der Anteil inkriminierter Angebote?

11. Ist der Bundesregierung bekannt, aus welchem Grund verschiedene Provider aufgefordert wurden, den Zugang zu Informationsangeboten zu unterbinden, und durch welche spezifischen technischen Maßnahmen wurde dies realisiert?

12. Auf welcher Rechtsgrundlage wurde dies durchgeführt?

13. Inwieweit verträgt sich die Unterdrückung eines Zugangs zu Daten und Nachrichten – jeweils betrachtet als Individualkommunikation wie als Massenkommunikation – mit bestehenden internationalen Abkommen und völkerrechtlich verbindlichen Verträgen, insbesondere der Europäischen Menschenrechtskonvention und ihrer Zusatzprotokolle, und wo setzen diese Abkommen Grenzen?

14. Welche Unterschiede im Recht zwischen den Staaten der EU und zwischen der Bundesrepublik Deutschland und den USA gibt es in für Computernetze relevanten Bereichen wie Meinungsäußerung, Informationszugang, Computerbetrug, Datenschutz, und welche Konsequenzen hat dies für die Strafverfolgung?

15. Welche Möglichkeiten stehen Staatsanwälten in der Bundesrepublik Deutschland offen, die Verbreitung links- wie rechtsextremistischer Texte in Ländern der EU und dabei speziell den Niederlanden und Dänemark zum einen in schriftlicher und zum anderen in elektronischer Form zu verfolgen?

    Sieht die Bundesregierung insoweit einen Handlungsbedarf?

16. Sind Polizeibehörden in den USA zur Unterstützung von bundesdeutschen Behörden bei der Verfolgung von Verbreitung einerseits kinderpornographischer und andererseits rechtsextremistischer Inhalte verpflichtet?

    Wenn ja, in wie vielen Fällen wurde diese Unterstützung gegeben?

    Wenn nein, sind Vereinbarungen über eine entsprechende Verpflichtung geplant?

17. Hat es bei der Verbreitung kinderpornographischer Inhalte sowohl in elektronischer als auch in nicht-elektronischer Form eine Zusammenarbeit bundesdeutscher und amerikanischer Strafverfolgungsbehörden gegeben?

Wenn ja, in welchem Umfang, in welcher Zahl, und zu wie vielen Strafverfahren ist es dadurch gekommen?

18. Hat es nach Kenntnis der Bundesregierung auf internationaler Ebene eine Abstimmung über die Unterstützung des von den USA inzwischen erlassenen Communications Decency Act gegeben?

    Wenn ja, sind Polizeibehörden in der Bundesrepublik Deutschland zur Unterstützung bei der Verfolgung von Straftaten gemäß dem von den USA erlassenen Communications Decency Act verpflichtet?

19. Auf welchen Bereich einer Rechtsangleichung im Zusammenhang mit elektronischer Kommunikation beziehen sich die von der Bundesregierung angekündigten Bestrebungen, internationale Regelungen durchzusetzen, und welche Regelungen strebt sie an?

20. Welche bestehenden Rechtsnormen sind nach Ansicht der Bundesregierung geeignet, das durch kommunikationstechnische Einrichtungen realisierte Zustandekommen eines Zugangs zu Daten und Informationen – differenziert nach Telekommunikations-Verbindungen zu Zwecken der Sprachtelefonie, des Fernkopierens, der Computerkommunikation und der Nutzung weiterer Dienste – zu unterbinden?

21. Unter welchen Voraussetzungen hält die Bundesregierung es für zulässig, den Zugang zu Daten und Informationen

    a) per Telefon,

    b) per Fax,

    c) per direkter Datenfernübertragung und

    d) im Internet

    zu unterbinden?

22. In welchen Bereichen sieht die Bundesregierung die Notwendigkeit, die dazu bestehende Gesetzeslage zu erweitern, und wie will sie dies umsetzen?

23. Sieht die Bundesregierung in einer Selektion und Kontrolle von Informationszugängen eine Gefährdung der grundrechtlich geschützten Freiheit der Bürgerinnen und Bürger, sich aus öffentlich zugänglichen Quellen umfassend zu informieren, und teilt die Bundesregierung die Auffassung, daß weltweit das Recht auf Informationsfreiheit gestärkt werden muß?

24. Welche Kosten erwachsen nach Ansicht der Bundesregierung den Anbietern von Telekommunikationsdienstleistungen durch die Aktivitäten der Strafverfolgungsbehörden einerseits und durch Auflagen zur Telefonüberwachung andererseits?

25. Sind der Bundesregierung Fälle bekannt geworden, in denen deutsche Provider durch das Eingreifen der Strafverfolgungs-

behörden in ihrer Konkurrenzfähigkeit bzw. wirtschaftlichen Existenz gefährdet werden?

Wenn ja, welche?

Bonn, den 12. April 1996

Dr. Manuel Kiper
Joseph Fischer (Frankfurt), Kerstin Müller (Köln) und Fraktion



Druck: Thenée Druck, 53113 Bonn, Telefon 91781-0
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon (02 28) 3 82 08 40, Telefax (02 28) 3 82 08 44
ISSN 0722-8333